

[REDACTED]

UNITED STATES OF AMERICA

v.

Manning, Bradley E.
PFC, U.S. Army,
HHC, U.S. Army Garrison,
Joint Base Myer-Henderson Hall
Fort Myer, Virginia 22211

Prosecution Motion

for Preliminary Determination of
Admissibility of Evidence
(Computer-Generated Records)

3 August 2012

(U) RELIEF SOUGHT

(U//FOUO) The prosecution in the above case respectfully requests that this Court admit into evidence the following account information and logs in advance of trial: Open Source Center (OSC) log files for the accounts bmannings and bradass87; OSC user information screenshots for the accounts bmannings and bradass87; Intelink logs showing activity for IP addresses (b) (7)(E) and (b) (7)(E) and the Intelink Passport account information for the account bradley.e.manning. The prosecution seeks said relief to provide improved predictability and efficiency to the proceedings.

(U) This motion also serves as notice to the defense that the government intends on offering these documents as evidence under Military Rule of Evidence (MRE) 902(11).

(U) BURDEN OF PERSUASION AND BURDEN OF PROOF

(U) The burden of proof on any factual issue, the resolution of which is necessary to decide a motion, shall be by preponderance of the evidence. RCM 905(c)(1). The burden of persuasion on any factual issue, the resolution of which is necessary to decide a motion, shall be on the moving party. RCM 905(c)(2). The United States has the burden of persuasion as the moving party.

(U) FACTS

(U) U.S. Army IP address [REDACTED] (hereinafter [REDACTED]) was the Accused's primary SIPRNET computer at his work station in the Sensitive Compartmented Information Facility (SCIF) at FOB Hammer, Iraq. See Enclosure 1. U.S. Army IP address [REDACTED] (hereinafter [REDACTED]) was the Accused's secondary SIPRNET computer at his work station in the SCIF at FOB Hammer. See Enclosure 2.

(U//FOUO) The Accused had an Intelink passport account. Intelink passport accounts have user names and passwords, and the Accused was assigned the user name bradley.e.manning. See Enclosures 4 and 9. The email address [REDACTED] was assigned to the account, and the account was last used on 27 April 2010. See Enclosure 4.

[REDACTED]

1

[REDACTED]

APPELLATE EXHIBIT 246
PAGE REFERENCED:
PAGE ___ OF ___ PAGES

[REDACTED]

(U) The Intelink passport account profile contains the identifying information of the user as well as personalized information in the form of questions and answers. See Enclosure 9.

[REDACTED]

(U) Intelink is the central SIPRNET search engine, analogous to www.google.com. While an Intelink search is the equivalent of an Internet Google search, Intelink searches websites only available via the SIPRNET. Searches using Intelink are typically logged. See Enclosure 3.

(U//FOUO) The Intelink log files revealed communications between the Accused's IP addresses in Iraq (b) (7)(E) and the Intelink servers. See Enclosure 3. The Intelink logs captured search terms that were searched on SIPRNET, as well as files that were downloaded. See Enclosures 3 and 8.

[REDACTED]

(U) The significance of the searches for "julian+assange" is that Julian Assange was the co-founder and head spokesman of Wikileaks.org. The significance of the searches for "iceland" is that on 18 February 2010, Wikileaks.org posted a classified Department of State cable from the U.S. Embassy in Reykjavik, Iceland. See Enclosure 3. The significance of the searches relating to cracking passwords was that in recovered chat logs on the Accused's personal computer, the Accused discussed using the same password cracking tools. The significance of the searches relating to TOR is that TOR is a distributed network of virtual tunnels that allows users to hide their actions while on the Internet and was used on the Accused's personal computer. See Enclosure 3. The significance of the "collateral murder," "reuters," or "12 Jul 07" searches is that Collateral Murder was the name given to a movie created by WikiLeaks.org and released on 5 April 2010 concerning an Apache helicopter air strike involving the death of a Reuter's reporter in 2007. See Enclosure 3.

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

(U) The OSC user account bradass87 was tied to the SIPRNET email address (b) (7)(E) [REDACTED] and was last used on 17 April 2010. See Enclosures 4 and 6. The Accused's AOL Instant Messenger username was bradass87. See Enclosure 4. The OSC account bmanning was tied to the SIPR email address bradley.manning@2bct10mtn and was last used on 6 November 2009. See Enclosures 4 and 5.

[REDACTED]

(U//FOUO) Between 17 March 2010 and 22 March 2010, the Accused's user account on his .22 computer accessed the files redcell_afghanistan.pdf and redcell_us_exporter_terrorism.pdf, both located in the folder C:\Documents and Settings\bradley.manning\My Documents\blah\ See Enclosure 4.

(U//FOUO) A user of the Accused's personal computer accessed a CD/DVD named 100322_1255 which contained the file blah.zip. The Accused's primary SIPRNET computer was configured to burn CD/DVDs and label them in a manner of YYMMDD_HHMM. See Enclosure 4.

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

(U) WITNESSES/EVIDENCE

(U) The prosecution requests the Court consider the following: Charge Sheet and Listed Enclosures.

(U) LEGAL AUTHORITY AND ARGUMENT

(U) The trial judge has discretion as to the manner in which she makes preliminary determinations concerning the admissibility of evidence. MRE 104; see U.S. v. Blanchard, 48 M.J. 306 (C.A.A.F. 1998). This judicial discretion includes "preadmitting" evidence provided it is relevant and no other rule prohibits its admission. See, e.g., U.S. v. Bradford, 68 M.J. 371 (C.A.A.F. 2010). Where, as here, there is no question as to the admissibility of the evidence, the enclosed computer-generated records should be preadmitted to provide predictability to both parties and to dispose of what amounts to administrative matters outside the presence of the panel (assuming there is a panel).

I. (U) THE RECORDS ARE RELEVANT.

(U) Evidence that has a tendency to make a fact of consequence more or less probable than it would be without the evidence is relevant. MRE 401. All relevant evidence is generally admissible. MRE 402.

A. (U) OSC Logs and User Account

(U) The OSC user account information reveals that bradass87 and bmannig were the Accused's user accounts, and the OSC logs show the Accused's activity on OSC.

[REDACTED]

B. (U) Intelink Logs and Intelink Passport Account

(U//FOUO) The Intelink Passport Account information is relevant to all the charged misconduct because it reveals that the bradley.e.manning account was set up and utilized by the Accused. See Enclosure 9.

[REDACTED]

[REDACTED]

(U) The Intelink logs are relevant to proving the charged misconduct in all the charges. They establish searches by the Accused for terms relating to all the charged misconduct. See Enclosure 8.

II. (U) THE RECORDS ARE NOT EXCLUDABLE AS HEARSAY BECAUSE THEY ARE COMPUTER-GENERATED ACTIVITY.

(U) Hearsay is an out-of-court statement, written or oral, offered for the truth of the matter asserted. MRE 801(c). A statement is an oral or written assertion or the nonverbal conduct of a person, if it is intended by the person as an assertion. MRE 801(a). A declarant is a person who makes a statement. MRE 801(b). A person must make a statement for it to be hearsay; a machine, therefore, cannot make a statement. See also Appellate Exhibit CCXVI ("machine generated data and printouts are not statements and, thus, they are not hearsay").

(U) United States v. Blazier, 69 M.J. 218 (C.A.A.F. 2010) is instructive on distinguishing between hearsay and computer generated records. In reviewing what portions of a drug testing report were admissible in a wrongful use case, the Court determined that testimonial hearsay included a signed, certified cover memorandum prepared at the request of the government for use at trial in which a person summarized the lab analyses. Id. at 221 fn.1. A person had written out what tests were conducted, what substances were detected, and the levels of each substance detected. Id. at 226. The cover memorandum was a written summary of the testimony that would be offered on the drug testing and its results.

(U) The Blazier Court then distinguished the testimonial hearsay in the cover memorandum from machine-generated records, such as raw data and calibration charts, stating: "it is well-settled that under both the Confrontation Clause and the rules of evidence, machine-generated data and printouts are not statements and thus not hearsay—machines are not declarants—and such data is therefore not 'testimonial.'" Id. at 224 (citing United States v. Lamons, 532 F.3d 1251, 1263 (11th Cir. 2008); United States v. Moon, 512 F.3d 359, 362 (7th Cir. 2008); United States v. Washington, 498 F.3d 225, 230-31 (4th Cir. 2007); United States v. Hamilton, 413 F.3d 1138, 1142-43 (10th Cir. 2005); United States v. Khorozian, 333 F.3d 498, 506 (3d Cir. 2003)). According to the Court, "[m]achine-generated data and printouts such as those in this case are distinguishable from human statements, as they 'involve so little intervention by humans in their generation as to leave no doubt they are wholly machine-generated for all practical purposes.'" Blazier, 69 M.J. at 224 (quoting Lamons, 532 F.3d at 1283 n.23).

(U//FOUO) Since the OSC logs and user account information screenshots, as well as the Intelink logs and Passport Account information are computer-generated, and thus not made by people, they cannot be hearsay.

[REDACTED]

III. (U) THE RECORDS ARE AUTHENTIC.

(U) In addition to being relevant, evidence must also be authentic to be admissible. See MRE 901(a). "[A]dmissibility is satisfied by evidence sufficient to support a finding that the matter in question is what its proponent claims." MRE 901(a). Some evidence, however, is self-authenticating and does not require "[e]xtrinsic evidence of authenticity as a condition precedent to admissibility." MRE 902. "Certified domestic records of regularly conducted activity" fall under this exception. MRE 902(11).

(U) Pursuant to MRE 902(11), extrinsic evidence of authenticity as a condition precedent to admissibility is not required with respect to certified domestic records of a regularly conducted activity when:

[t]he original or a duplicate of a document or record of regularly conducted activity that would be admissible under Mil R. Evid. 803(6) if accompanied by a written declaration of its custodian or other qualified person, in a manner complying with any Act of Congress or rule prescribed by the Supreme Court pursuant to statutory authority certifying that the record (A) was made at or near the time of the occurrence of the matters set forth by, or from information transmitted by, a person with knowledge of those matters; (B) was kept in the course of the regularly conducted activity; and (C) was made by the regularly conducted activity as a regular practice.

MRE 902(11).

(U) "Records of regularly conducted activity" is defined in MRE 803(6) as the following:

[a] memorandum, report, record, or data compilation, in any form, of acts, events, conditions, opinions, or diagnoses, made at or near the time by, or from information transmitted by, a person with knowledge, if kept in the course of a regularly conducted business activity, and if it was the regular practice of that business activity to make the memorandum, report, record, or data compilation, all as shown by the testimony of the custodian or other qualified witness, or by certification that complies with Mil. R. Evid. 902(11) or any other statute permitting certification in a criminal proceeding in a court of the United States, unless the source of the information or the method or circumstances or preparation lack trustworthiness.

MRE 803(6).

[REDACTED]

[REDACTED]

(U) The following attestations were made for the enclosed computer-generated files:

(U//FOUO) On 22 June 2012, (b) (7)(C) [REDACTED] National Security Agency, Fort Meade, MD, attested to the authenticity of the Intelink logs for both the computer used by the Accused in Iraq and the Intelink Passport account information for the Accused. Specifically, (b) (7)(C) [REDACTED] attested to the following: the listed logs for IP address (b) (7)(E) [REDACTED] with date ranges of 9 November 2009 to 30 December 2009, 23 January 2010 to 11 February 2010, and 2 March 2010 to 12 May 2010; the listed logs for IP address (b) (7)(E) [REDACTED] with date ranges of 9 November 2009 to 31 December 2009, 1 January 2010 to 28 February 2010, and 1 March 2010 to 21 May 2010; and the Intelink Passport account information for (b) (7)(E) [REDACTED] contained in the file manning.Idif. See Enclosure 6.

(U//FOUO) On 29 June 2012, (b) (7)(C) [REDACTED] Central Intelligence Agency, Washington, DC, attested to the authenticity of the OSC log files and user information files, specifically for those OSC accounts pertaining to the users bradass87 and bmanning. See Enclosure 7.

(U) Since the attestations accompanying all records were made in accordance with MRE 902(11), all the records are properly authenticated.

IV. (U) THE RECORDS ARE IN A FORM THAT IS BEING OFFERED AS AN ORIGINAL OR DUPLICATE UNDER THE ORIGINAL WRITING RULE, OR THERE IS ADMISSIBLE SECONDARY EVIDENCE TO PROVE THE CONTENTS OF THE RECORDS IAW MRE 1001-1008.

(U) "A duplicate is admissible to the same extent as an original unless (1) a genuine question is raised as to the authenticity of the original, or (2) in the circumstances it would be unfair to admit the duplicate in lieu of the original." MRE 1003. A duplicate is defined as "a counterpart produced by the same impression as the original, or from the same matrix, or by means of photography, including enlargements and miniatures, or by mechanical or electronic rerecording, or by chemical reproduction, or by other equivalent techniques which accurately reproduce the original." MRE 1001(4). "The contents of an official record . . . including data compilations in any form, if otherwise admissible, may be proved by copy, certified as correct or attested to in accordance with Mil. R. Evid. 902 or testified to be correct by a witness who has compared it with the original. If a copy which complies with the foregoing cannot be obtained by the exercise of reasonable diligence, then other evidence of the contents may be given." MRE 1005.

(U) In the certifications for all of the enclosed records, the records custodian specifically states that the records are true and accurate or complete copies of the originals. There is no evidence that any of the original documentation may not be authentic, nor is there any circumstance present which would make the admission of a duplicate in lieu of the original unfair. The enclosures include official records, and all of them are business records. The duplicates, therefore, are admissible to the same extent as the originals.

[REDACTED]

V. (U) THE PROBATIVE VALUE OF THE RECORDS IS NOT SUBSTANTIALLY OUTWEIGHED BY UNFAIR PREJUDICE.

(U) Courts may exclude relevant evidence if its probative value is substantially outweighed by the danger of unfair prejudice, confusion, or waste of time. MRE 403. Prejudice alone is not sufficient to warrant exclusion. Virtually all evidence is prejudicial to one party or another. To justify exclusion the prejudice must be unfair. United States v. Candelaria-Silva, 162 F.3d 698, 705 (1st Cir. 1998).

(U) In the instant case, the log records and user account information are extremely probative in that they track what was occurring on the computers used by the Accused and on the user profiles created by the Accused. The evidence is prejudicial to the Accused in that it builds the case against him; however, it is not unfairly prejudicial. All of the logs are relevant to the Accused and the charged offenses and are a direct result of the Accused's actions. The logs establish a timeline to make the events clear to the factfinder.

CONCLUSION

(U) Based upon the requirements for admissibility of evidence in accordance with MRE 104, MRE 401, MRE 402, MRE 403, MRE 801, MRE 803(6), and MRE 902(11), the Government respectfully moves this Court, pursuant to RCM 906(13) to pre-admit the OSC logs and user information and the Intelink logs and user information in Enclosures 5-9 because they are relevant to the charges at issue and computer-generated information. They will provide improved predictability and efficiency to the proceedings.



ANGEL M. OVERGAARD
CPT, JA
Assistant Trial Counsel



(U) I certify that I served or caused to be served a true copy of the above on Defense Security Experts, via electronic mail, on 3 August 2012.



ANGEL M. OVERGAARD
CPT, JA
Assistant Trial Counsel

(U) 9 Enclosures

[REDACTED]

- 
1. (U) Forensic Report MANNING SIPR 22.225.41.22-22 Sep 11 (attached to AE CLXXVIII as Enclosure 1)
 2. (U) Forensic Report MANNING SIPR 22.225.41.40-22 Sep 11 (attached to AE CLXXVIII as Enclosure 2)
 3. (U) Forensic Report Intelink Logs-22 Sep 11
- 

5. (U) OSC User Information Files (bmanning) with attestation
6. (U) OSC User Information Files (bradass87) with attestation
7. (U) OSC Logs (bmanning & bradass87) with attestation
8. (U) Intelink .22 & .40 Logs with attestation
9. (U) Intelink Passport Account Information with attestation

UNCLASSIFIED//FOUO

V.

**Prosecution Motion
For Preliminary Determination of
Admissibility of Evidence
(Computer-Generated Records)**

Enclosures 5-6

3 August 2012

See Attached CD

ATTESTATION CERTIFICATE

This document is intended to meet the requirements set forth in Military Rules of Evidence Rule 902(11), addressing certified records of regularly conducted activity.

I swear or affirm that each of the following is true regarding the attached records, to the best of my knowledge and belief:

1. I am the custodian of these records, or I am an employee familiar with the manner and process in which these records are created and maintained, by virtue of my duties and responsibilities;
2. The records were made at or near the time of the occurrence of the matters set forth by, or from information transmitted by, a person with knowledge of these matters;
3. The records were kept in the course of regularly conducted business activity;
4. The records were made by the regularly conducted activity as a regular practice; and
5. The records are a true, accurate, and complete copy of the original documents.

List of attached records:

OSC log files, containing the following logs, with the following date ranges:

bmanning_distinct_export_with_classification.xls	6-Nov-09 - 9-Nov-10
bradass87_distinct_export_with_classification.xls	20-Feb-10 - 17-Apr-10
bradass87_sum_export_with_classification.xls	No date range

OSC user information files entitled:

Opensource.gov-bmanning.pdf
Opensource.gov-bradass87.pdf

Organization: Central Intelligence Agency

Signature (b) (7)(C)

Date

6/29/2012

Print or Type Name

(b) (7)(C)

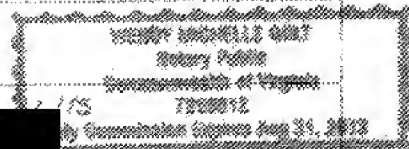
Title

DRA/

Owens

Business Address

(b) (6)



Subscribed and sworn to before a notary public, this 29 day of June, 2012

Notary Public

My commission expires on:

8-31-2013



- 5. OSC User Information Files
(bmanning)
- 6. OSC User Information Files
(bradass87)